监控EIGRP在连结7000上的邻接变化的SNMP陷阱

目录

概述

连结只支持EIGRP-MIB的两个陷阱， cEigrpAuthFailureEvent和cEigrpRouteStuckInActive，但是up/down的EIGRP邻居的没有SNMP陷阱(cEigrpNbrDownEvent)。
形成SNMP陷阱的一可行的应急方案监控EIGRP邻接更改是配置-一个邻居的和一个下来邻居的-被触发的两份EEM脚本基于Syslog模式。

示例

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

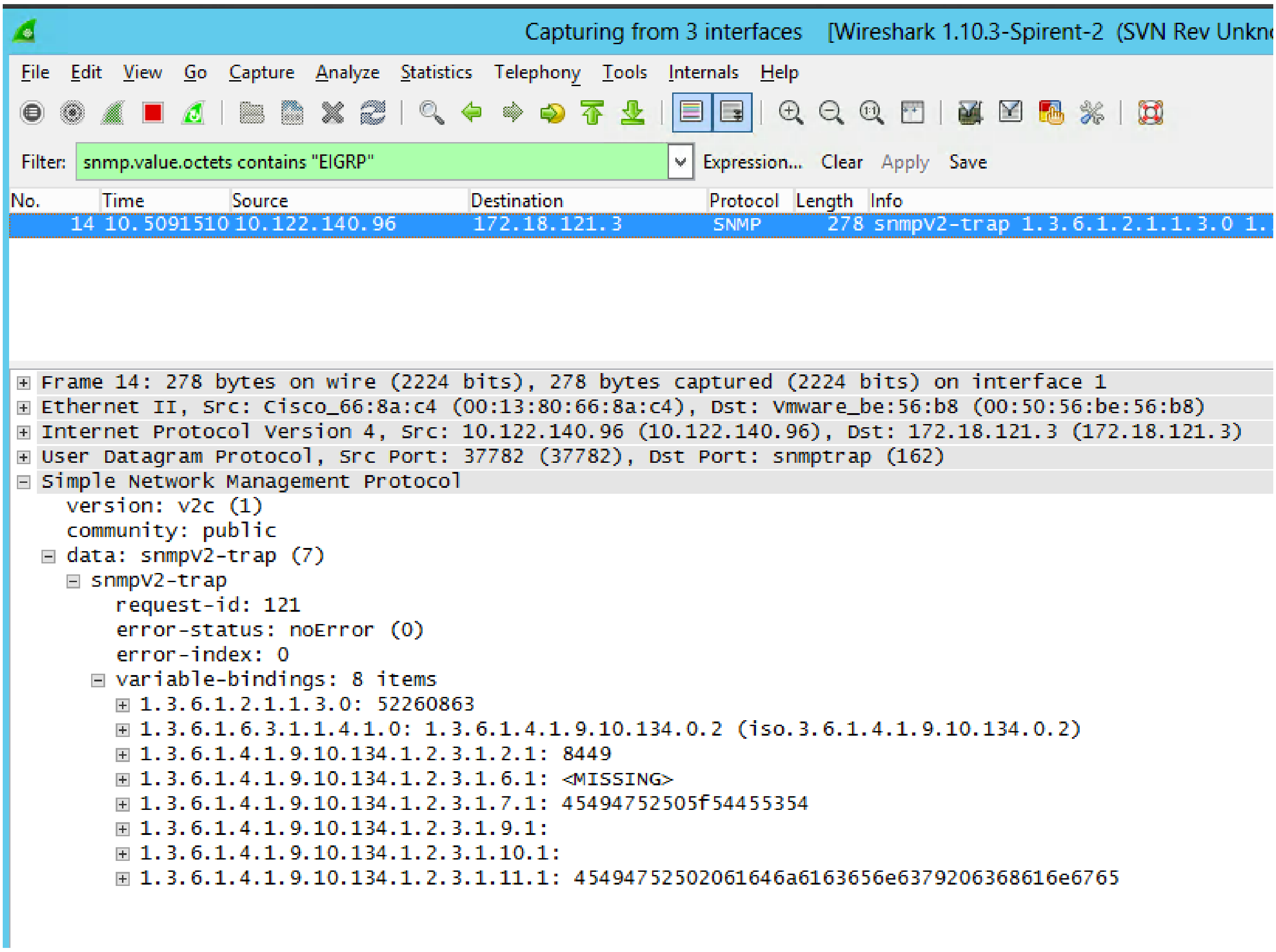
您能由飘荡然后测试第3层接口(您可以创建测验SVI验证至于不打乱连接)：

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

确认连结通过检查您的SNMP监控工具发送这些正确地-输出可能根据使用的工具轻微有所不同：

您可以通过Wireshark捕获也查看这些SNMP陷阱：

注意：*根据Wireshark版本，字符串不会在人类易读的文本，然而可以通过"snmp.value.octets被过滤包含"EIGRP ""*



您能也验证连结发送这些在触发与Ethanalyzer的EEM -示例：

```
N7K-A-Admin# ethanalyzer local interface mgmt display-filter snmp limit-c 0

Capturing on mgmt0
2017-07-12 15:43:37.431067 10.122.140.96 -> 172.18.121.3 SNMP 278 snmpV2-trap 1.3.6.1.2.1.1.3.0
1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1
1.3.6.1.4.1.
9.10.134.1.2.3.1.7.1 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1
```

注意：前NX-OS 7.x不给出我们配置“反之将允许您监控整个记录日志日志为EIGRP消息然后过滤的**snmp-server enable traps Syslog的**”选项。此功能在最新版本被添加了，7.x和以后。